Identités biométrisées et contrôle social

François PELLEGRINI, André VITALIS

RESEARCH REPORT
N° 9046
Mars 2017
Project-Team TADAAM

ISSN 0249-6399 ISRN INRIA/RR--9046--FR+ENG

Identités biométrisées et contrôle social

François Pellegrini *, André Vitalis †

Équipe-Projet TADAAM

Rapport de recherche n° 9046 — Mars 2017 — 12 pages

Résumé : Pour assurer l'identité des personnes, deux approches complémentaires ont été poursuivies : la numérotation et la biométrie. En permettant leur usage conjoint à faible coût, les technologies numériques ont créé les conditions de leur déploiement à grande échelle. Celui-ci, maintes fois repoussé en France, a été effectivement engagé à l'occasion du tournant sécuritaire de la fin du XXe siècle. L'usage des technologies les plus récentes n'a cependant pas été accompagné d'un examen critique des architectures et procédures héritées du XIXe siècle. Cette réflexion doit absolument être menée, afin de garantir aux systèmes mis en œuvre des caractéristiques permettant qu'ils ne soient pas détournés contre la population en cas de troubles majeurs de la société.

Mots-clés : numérotation des individus, biométrie, authentification, identification, architecture des systèmes, falsification.

* Professeur d'informatique, université de Bordeaux, francois.pellegrini@labri.fr

† Professeur émérite de sciences de l'information et de la communication, Université Bordeaux Montaigne, andre.vitalis@msha.fr

RESEARCH CENTRE
BORDEAUX – SUD-OUEST

200, avenue de la Vieille Tour
33405 Talence Cedex

Biometrized identities and social control

Abstract: Two complementary approaches have been pursued to ensure the identity of people: numbering and biometrics. By allowing their joint use at low cost, digital technologies have created the conditions for their large-scale deployment. This deployment, which had been rejected at several occasions, started in France in the context of the security turn of the end of the twentieth century. However, this use of the most recent technologies has not been accompanied by a critical review of the architectures and procedures inherited from the nineteenth century. This reflection must absolutely be carried out in order to ensure that implemented systems possess characteristics that allow them not to be misused against the population in case of major social disorder.

Key-words: numbering of individuals, biometrics, authentication, identification, systems architecture, falsification.

1 Identifier un individu obéit à diverses raisons. On peut vouloir le connaître, le reconnaître, le compter mais aussi le surveiller, l'exclure voire le réprimer. Des historiens distinguent différents régimes d'identification qui se sont succédés au cours du temps [1, 14]. Le plus ancien est fondé sur l'oralité et les relations interpersonnelles de face à face. Ensuite, avec la mobilité accrue des populations et l'affirmation du pouvoir étatique, apparaissent des techniques d'identification à distance qui vont construire une identité de papier où le nom patronymique est consigné dans un écrit. Sous-tendue par un recours massif à l'informatique [13], on observe, à l'époque contemporaine, une rationalisation des procédés d'identification doublés par des procédés d'authentification.

2 Les différentes modalités et techniques d'identification comportent d'importants enjeux politiques et techniques. On peut estimer par exemple, que désigner un individu par un numéro unique en le coupant de sa généalogie et de ses racines, porte atteinte à sa qualité d'être humain. C'est précisément le projet SAFARI de croisement de toutes les données sociales disponibles sur les individus au moyen d'un numéro de ce type, au début des années 1970, qui est à l'origine d'un débat public sur les dangers d'une identité numérotée et informatisée [18]. Ce débat devait déboucher en 1978 sur le vote d'une loi relative à l'informatique, aux fichiers et aux libertés, qui limite l'utilisation de ce numéro. Dans son article premier, elle proclame que : « *L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, à la vie privée, ni aux libertés individuelles et publiques* ».

3 Aujourd'hui, l'informatisation des données biométriques de toute la population française par le méga-fichier TES (Titres électroniques sécurisés), créé en octobre 2016, permet une authentification des titulaires de titres d'identité mais également, comme l'autorise la numérotation, une identification unique d'autant plus irrévocable qu'elle est portée par le corps même de l'individu. Une opération d'une telle portée, ordonnée par un simple décret, met en péril les valeurs proclamées par la loi de 1978 révisée en 2004 et les objectifs qu'elle se fixe. Une préoccupation sécuritaire omniprésente fait oublier la puissance de contrôle de l'informatique et les dangers d'une identification rigide et centralisée, tout en écartant d'autres solutions plus respectueuses des autonomies individuelles.

1 Des projets d'informatisation de l'identité refusés au nom des libertés

4 La rationalisation contemporaine des modalités d'identification des individus a emprunté deux voies principales : la numérotation et la biométrie. L'informatisation conjointe de ces deux types d'identification suscitera une prise de conscience accrue de leurs dangers pour les libertés et les autonomies individuelles.

5 Le recours à un numéro unique dans la désignation d'un individu présente l'avantage d'une désignation sans ambigüité. À un numéro ne correspondra par définition qu'un individu alors qu'un nom, même associé à un prénom, ne permet pas d'identifier une personne avec certitude. C'est au sein d'institutions fondées sur une obéissance absolue comme les prisons ou l'armée que les pratiques d'identification numérotée s'imposent en premier. Un exemple paroxystique est évidemment celui des camps de concentration nazis, où l'emploi du numéro, à l'exclusion de tout autre identification, servait une volonté de dépersonnalisation intégrale.

À côté du nom patronymique, les États vont avoir recours à la numérotation de leurs populations pour assurer une certification de l'identité. En France, la création d'un numéro national d'identité remonte aux années 1940-41 [11]. Cette numérotation, mise en œuvre dans des conditions très difficiles avec des objectifs patriotiques et militaires qui seront cachés à l'occupant, sera utilisée par la suite par l'État-Providence et la Sécurité sociale. À travers les services rendus

dans l'identification des individus, elle se banalisera et s'imposera bientôt comme une nécessité de gestion.

Au début des années 1970, l'informatisation du répertoire des numéros tenu par l'INSEE, sous le nom de projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus), va être à l'origine d'une polémique de grande ampleur, à la suite des révélations de la presse. À l'occasion de son informatisation, on entend faire jouer au numéro un nouveau rôle fédérateur entre les différents fichiers. Comme le précise une note officielle, « L'objectif visé est de rendre possible une diffusion massive du numéro INSEE dans l'administration, voire hors de l'administration (banques, assurances...) et de généraliser ainsi son utilisation, ce qui permettrait de le rendre obligatoire ». Concrètement, il s'agissait d'organiser, à partir de ce numéro unique à la disposition de tous les ficheurs, l'interconnexion des différents fichiers informatisés concernant un individu. 6

Une réaction démocratique devant un tel danger pour les libertés ne s'est pas faite attendre : interdiction d'interconnecter des fichiers de ministères différents, nomination d'une commission de sages, vote d'une loi en 1978 qui donna naissance à la CNIL, mettant à la charge des ficheurs des obligations nouvelles et attribuant de nouveaux droits aux personnes fichées. L'informatique, en rendant plus efficace la numérotation des personnes, a contribué à faire apparaître au grand jour ses potentialités de contrôle et leurs dangers pour les libertés individuelles.

Dans le dernier tiers du XIXe siècle, l'identification judiciaire a servi de laboratoire pour expérimenter de nouvelles techniques destinées à améliorer la reconnaissance des individus. Les mesures du corps préconisées par l'anthropométrie d'Alphonse Bertillon seront effectuées jusqu'au début des année 1930 et complétées par la prise des empreintes digitales recommandée par la dactyloscopie [3, 12, 16]. L'instauration en 1912 d'un carnet anthropométrique pour les populations nomades est une date importante, à partir de laquelle est imposé à des familles entières un document d'identification réservé jusqu'alors aux prisonniers et aux criminels. Les administrations coloniales imposeront également ces mêmes documents aux populations subalternes de la société indigène. Par le biais d'une carte d'identité, l'identification administrative va être étendue progressivement et concerner bientôt toute la population des « gens honnêtes ». En 1917, ce sont les étrangers qui doivent s'inscrire auprès des services préfectoraux et se voient imposer cette carte. En 1921, une carte est créée pour les habitants du département de la Seine, mais son extension à tout le territoire fait débat. Des opposants à cet encartement, auquel les grandes démocraties anglo-saxonnes ont refusé de recourir, le dénoncent comme un outil transformant les citoyens en suspects. C'est à la faveur de la débâcle de 1940 que le gouvernement de Vichy crée une carte d'identité de Français obligatoire. Supprimée à la fin de la guerre, cette carte est rétablie en 1955, au début des « événements d'Algérie », mais demeure facultative. En 1969, 75 % de la population l'ont adoptée, les procédures pour l'obtenir ayant été simplifiées. Une vérification de l'état-civil effectuée à l'échelle départementale est suffisante. 7

Il faut attendre les années 1970-1980 pour voir apparaître des projets d'informatisation de la carte d'identité. Un premier projet de carte informatisée est officialisé en 1980 mais est remis en cause quelques mois plus tard par le gouvernement socialiste qui vient d'arriver au pouvoir. En 1986, un gouvernement de droite propose un nouveau projet de « carte nationale sécurisée » qui prévoit un mode de production centralisé du titre et, surtout, la mise en place d'un Fichier national de gestion (FNG), consultable en temps réel par la police et la gendarmerie en tous points du territoire. La production d'une carte devenue une sorte de laissez-passer, à la faveur du vote d'une loi rendant obligatoire les contrôles d'identité, sera abandonnée à l'occasion d'une nouvelle conjoncture politique. 8

En 2005, un projet INES (Identification nationale électronique sécurisée) propose la création d'une carte d'identité biométrique articulée autour de fichiers nationaux, les empreintes digitales et les photos étant stockées dans des fichiers séparés. À la suite d'un débat organisé par le Forum

des droits sur l'Internet, au cours duquel de nombreuses critiques ont été émises, notamment en ce qui concerne la préservation des libertés individuelles, ce projet devait être également abandonné. L'informatisation des données biométriques de la population reste cependant un objectif gouvernemental toujours présent, comme le montre le vote en 2012 d'une loi relative à la protection de l'identité qui crée un fichier central d'empreintes biométriques. Pour parvenir à ce résultat, plusieurs difficultés ont du être surmontées. La loi trouve son origine dans une proposition parlementaire qui a écarté les objections de la CNIL, défavorable comme tous ses homologues européens à une centralisation des données biométriques. La lutte contre l'usurpation d'identité est mise en avant pour justifier la création d'un fichier biométrique permettant de valider les données contenues dans les cartes d'identité et les passeports mais qui sera mis également à la disposition de la police. Le Conseil constitutionnel, saisi quelques jours après le vote de la loi, devait censurer la disposition créant ce fichier qui, selon lui, porte une atteinte au droit à la vie privée qui n'est pas proportionnée à la finalité déclarée [8].

9 Tous les projets d'informatisation de la carte d'identité en changent la finalité. Les possibilités informatiques permettent de stocker les données personnelles, et en particulier les données biométriques, sous une forme centralisée mais aussi de les consulter à distance et pour tout autre chose que la validation des cartes. L'échec de différents projets présentés témoigne de la prise de conscience des possibilités liberticides de l'informatique, particulièrement en ce qui concerne l'informatisation biométrique et, face à ces dangers, de la volonté de préserver les libertés qui fondent une démocratie et la font vivre.

2 Un tournant securitaire servi par la puissance de contrôle de l'informatique

10 Les fichiers régaliens, notamment policiers, constituent une nécessité mais aussi une menace pour les libertés individuelles. Une démocratie doit toujours rechercher un équilibre et un compromis dans le couple libertés/sécurité. Ce n'est pas un hasard si l'État s'est longtemps abstenu dans la gestion des identités et a imposé une identité administrative aux seules populations délinquantes, marginales ou fragiles comme les nomades, les étrangers ou les colonisés. Progressivement, toute la population, même celle des « gens honnêtes », va être concernée par un encartement autoritaire en période de crise puis par un encartement libéral et décentralisé dans un contexte démocratique retrouvé. À partir des années 1970, l'informatique trouble ce jeu en permettant de convertir les identifications administratives en outils de contrôle des populations. Afin de rétablir un équilibre compromis dans le couple libertés/sécurité par le recours à une technique potentiellement liberticide, un certain nombre de règles ont été posées par la loi pour la création et la gestion des fichiers informatisés : finalité, proportionnalité, durée de conservation des informations, contrôle d'une commission indépendante. L'utilisation du numéro INSEE a été cantonnée au secteur social, les différentes administrations devant recourir à des numéros spécifiques. Pour les mêmes raisons, tous les projets d'informatisation de la carte d'identité ont été repoussés. Il n'est pas question d' entraver l'informatisation, considérée comme un gage de progrès économique et social, mais on souhaite qu'elle respecte les libertés et l'intimité de la vie privée, sans trop se demander si cela est effectivement possible.

11 La recherche d'un équilibre dans le couple libertés/sécurité va s'avérer de plus en plus délicate au cours du temps, le souci sécuritaire prenant le pas sur toute autre considération [19]. La sécurité va être formulée, en des termes nouveaux, comme un droit fondamental de l'individu que l'État se doit de faire respecter. Une telle formulation fragilise un droit naturel et imprescriptible, le droit à la sûreté, inscrit dans la Déclaration des droits de l'Homme et du citoyen de 1789, qui protège l'individu contre un arbitraire toujours possible de l'État, considéré bien plus comme un

problème que comme une solution [10].

Dans la prédominance d'un souci sécuritaire, le 11 septembre 2001 marque un tournant essentiel. À partir de cette date, au nom d'une lutte contre un terrorisme qui se joue des frontières, les États-Unis vont promouvoir et imposer à leurs alliés, spécialement européens, leurs conceptions et leurs pratiques en matière de contrôle des identités et des mouvements. Ce pays considère que, couplée avec l'informatique, la biométrie qui assure la reconnaissance d'un individu à partir de certaines caractéristiques corporelles, constitue un identifiant sûr et universel. Le *Patriot Act* impose, pour entrer sur le territoire étasunien, l'usage d'un passeport biométrique sécurisé lisible en machine, en particulier aux 27 pays dispensés jusqu'alors de visa. La date limite de sa mise en œuvre, fixée en 2004, sera repoussée pour des raisons essentiellement techniques. L'Union européenne et les États qui la composent se plient à ces exigences étasuniennes d'autant plus facilement qu'ils avaient eux-mêmes retenu les techniques biométriques dans leur lutte contre l'immigration clandestine et les actes criminels. La base de données VIS (*Visa Indentification System*) enregistre les données biométriques des demandeurs de visa à destination de l'Union, de même que le système d'information Schengen, dit SIS II, pour le contrôle aux frontières des personnes signalées. Le fait que les États-Unis aient confié à l'Organisation de l'aviation civile internationale (OACI), dépendante de l'ONU, le soin de définir un standard biométrique unique, a facilité la conclusion d'un accord qui est intervenu en 2004.

La France n'aura guère de mal à s'aligner sur les exigences étasuniennes dans la mesure où, 12
dès le milieu des années 1990, elle a pris un tournant sécuritaire [5]. Toutefois, à partir du 11 septembre 2001, la préoccupation sécuritaire devient obsessionnelle. Cette date marque l'entrée en scène d'un État surveillant qui, au-delà des alternances politiques droite/gauche, n'aura de cesse de prendre des mesures restreignant les libertés au nom de la lutte contre le terrorisme. Les lois sur la sécurité convertissant les techniques d'information et de communication en techniques de contrôle vont se succéder à un rythme soutenu. Une loi du 21 novembre 2001 sur la sécurité quotidienne oblige les fournisseurs d'accès à l'Internet à conserver pendant un an les données de connexion de leurs abonnés. Une loi du 13 mars 2003 sur la sécurité intérieure rend cette obligation définitive. Une loi du 23 janvier 2006 relative à la lutte contre le terrorisme autorise l'accès sans mandat à ces données de connexion aux services anti-terroristes ainsi que le pistage des déplacements par géolocalisation et permet le développement de la vidéosurveillance dans les lieux publics. Une loi du 14 mars 2011 pour la performance de la sécurité intérieure, généralise le recours à cette technique. Une loi du 18 décembre 2013 sur la programmation militaire, légalise la surveillance de la totalité de l'Internet par la police sans l'intervention d'un juge. Une loi du 13 novembre 2014 sur le terrorisme renforce les moyens de lutte contre ce phénomène. Une loi du 24 juillet 2015 sur le renseignement élargit les buts des écoutes et légalise les techniques d'information intrusives utilisées par les services de renseignement.

Les fichiers de police se sont multipliés, créés pour la plupart par des actes réglementaires et sans le contrôle strict exercé jusqu'en 2004 par la Commission Informatique et libertés. Leur nombre passe approximativement de 35 en 2006, à 80 en 2015. Des finalités supplémentaires sont ajoutées au fur et à mesure aux finalités annoncées au départ. Ainsi, un méga-fichier STIC, créé à des fins d'enquêtes judiciaires, va être progressivement utilisé pour des enquêtes administratives de moralité en 2001, pour l'instruction des demandes de nationalité française en 2003 et pour des enquêtes visant des personnes candidates à un emploi public en 2005. Il en est de même pour un fichier FNAEG d'empreintes génétiques, créé en 1998 pour lutter contre les criminels sexuels récidivistes. Ce fichier sera étendu en 2003 aux auteurs des infractions les plus banales, puis transformé en 2016 en « fichier génétique des gens honnêtes »(voir *infra*). Dans ces conditions, le nombre de personnes fichées, qui atteint plusieurs millions, a constamment augmenté en même temps que les risques liés aux fichiers. Les défaillances dans la mise à jour de données conservées plus longtemps sont devenues de plus en plus fréquentes.

13 Au-delà des opérations ponctuelles de fichage ou de mise en place de dispositifs sécuritaires, on observe une véritable stratégie pour jeter les bases d'une nouvelle économie du contrôle qui réclame une amélioration de l'identification des individus et notamment l'informatisation des données biométriques de toute la population. Dans le contexte très particulier d'un état d'urgence maintenant installé depuis plus d'un an, après les nombreux échecs des projets visant à réaliser une telle opération, c'est ce à quoi réussit le méga-fichier TES.

Le méga-fichier TES a été présenté par le ministère de l'Intérieur comme le successeur, par nature plus moderne, de deux fichiers administratifs existants : le fichier servant à la gestion des passeports biométriques (appelé également TES, et que nous appellerons « TES-1 » pour le distinguer de son extension « TES-2 ») et le FNG servant à la gestion administrative des cartes d'identité. Les finalités annoncées d'un tel fichier, outre la mutualisation des moyens entre les deux dispositifs précédents, sont doubles : la gestion des titres et la lutte contre la fraude documentaire. Dès le moment où un titre est délivré à une personne donnée, il semble naturel de garder trace de l'émission dudit titre et de l'identité de la personne concernée, afin que cette dernière ne puisse pas demander plusieurs titres l'un après l'autre, qu'elle fournirait à d'autres personnes. De même, lorsqu'une personne se présente afin de faire renouveler son titre d'identité périmé, il est important de savoir si ladite personne est bien le titulaire de l'ancien titre ou bien un usurpateur. Ce pourrait par exemple être une personne qui, profitant d'une vague ressemblance avec le visage du titulaire (surtout lorsqu'on procède au renouvellement d'une carte ayant appartenu à un jeune adolescent dont le visage a changé), souhaiterait faire établir un nouveau titre avec sa propre photo. L'authentification des demandeurs, en particulier au moyen de la biométrie, fait donc partie des moyens de lutte contre la fraude documentaire. Cependant, elle n'y est pas réductible. Par exemple, l'insertion de dispositifs signés de façon cryptographique au sein des documents contribue grandement à la lutte contre la fraude, en rendant lesdits documents bien plus difficiles à contrefaire. Il faudrait en effet que les faussaires cassent le chiffrement de la signature de l'autorité émettrice pour pouvoir signer à leur tour les données d'identité figurant sur un tel support.

3 Les risques oubliés d'une identification administrative centralisée et univoque

14 La biométrie peut être employée à deux finalités distinctes : l'authentification et l'identification. L'authentification vise à déterminer si une personne est bien celle qu'elle prétend être. Pour cela, on compare les données biométriques de la personne avec celles qui ont été préalablement collectées de façon contrôlée auprès de la personne en question. Si les données correspondent, la personne est bien celle ayant cette identité ; sinon, c'est une autre personne, ayant une autre identité, sans que l'on puisse connaître laquelle. L'identification, pour sa part, vise à retrouver l'identité associée à une trace biométrique que l'on possède, qu'elle ait été collectée sur une scène de crime ou qu'elle ait été prélevée sur un cadavre inconnu ou une personne amnésique. On va alors comparer ladite trace avec l'ensemble des données biométriques contenues dans une base de référence, dans l'espoir de trouver une correspondance. Si une telle correspondance est trouvée, l'identité de la personne ayant laissé la trace est révélée ; sinon, c'est que ladite personne n'est pas présente dans le fichier.

15 La principale motivation du refus de mise en place d'un fichier biométrique centralisé au cours des vingt dernières années, a été le risque de détournement de finalité, pouvant conduire à ce qu'un fichier administratif constitué dans un but d'authentification soit utilisé à fin d'identification, en tant que fichier de police. C'est bien la menace que constitue, pour les libertés publiques, une telle base centrale d'identification biométrique de tous les Français, appelé lors des débats le « fichier

des gens honnêtes », qui avait conduit le Conseil constitutionnel à censurer en 2012 un précédent projet de modernisation du FNG [8]. Qui plus est, l'authentification biométrique ne nécessite aucunement le recours à une base centrale. Il suffit, pour la réaliser, que la personne ait en sa possession un document certifié par l'autorité émettrice, contenant ses gabarits biométriques sous une forme infalsifiable. C'est le cas par exemple lorsque lesdits gabarits sont cryptographiquement signés par l'autorité émettrice. Or, le choix opéré par le ministère de l'Intérieur dans le cas du fichier TES-2 a pourtant été de conserver les données biométriques des personnes dans une base centrale [6].

Il a suffi, pour mettre en œuvre ce fichier, d'un simple décret, sans que la question ne soit débattue devant le Parlement comme en 2012. Bien que ledit décret ait fait l'objet d'un avis extrêmement réservé de la CNIL, le Conseil d'État a validé le système TES-2, au motif que sa seule finalité annoncée était l'authentification et que le ministère de l'Intérieur garantissait que des barrières techniques empêcheraient l'usage du fichier pour l'identification, en ne permettant pas de remonter d'une empreinte biométrique aux informations nominatives. Ces arguments sont inopérants pour deux raisons. D'une part, les barrières techniques alléguées par le ministère de l'Intérieur peuvent être facilement contournées, car il est facile de reconstruire l'information de liaison entre les données biométriques et les identités [15] ; on peut facilement s'en convaincre, du simple fait que réaliser une identification revient à effectuer une tentative d'authentification avec chacune des personnes de la base centralisée, avec l'espoir que l'une d'entre elles réussisse. D'autre part, le décret TES-2 mentionne explicitement la possibilité de réquisitions judiciaires, sans que la nature de celles-ci soit explicitée. Puisqu'il est techniquement possible d'effectuer des identifications, un juge ne pourrait-il requérir de comparer les données biométriques du fichier avec celles issues d'une scène de crime ? Le décret TES-2 dispose également que les services de renseignement auront accès au fichier. Or, personne ne serait en mesure de contrôler l'usage par ces services d'une copie qu'ils en feraient pour leur propre usage. Toutes ces failles ont été confirmées, à mots à peine couverts, par l'audit conjoint du système TES-2 réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) [17].

16 À l'opposé d'une architecture centralisée et fortement contrôlée par un pouvoir central, un régime administratif libéral et décentralisé de certification des identités permet, en temps de crise, d'éviter bien des drames. C'est un régime de ce type qui a permis au cours de la dernière guerre, à des dizaines de milliers de personnes ayant eu la possibilité de changer de nom, d'échapper aux nazis [9]. Des faux papiers ont sauvé des résistants, des Juifs, des hommes politiques et des syndicalistes qui étaient recherchés. Ces faux papiers étaient fabriqués à partir de divers formulaires vendus dans le commerce qui, après avoir été renseignés, devaient être tamponnés dans une préfecture. Pour devenir une personne passant à travers les mailles des contrôles, il suffisait de disposer d'un faux tampon ou d'une complicité a l'intérieur de la préfecture. La seule vérification possible était de téléphoner à la commune d'origine pour consulter le registre des naissances, ce qui demandait beaucoup de temps et se révélait souvent inutile dans la mesure où le lieu de naissance indiqué était une mairie choisie pour avoir été bombardée et avoir perdu toute sa documentation. En créant en 1940 une carte d'identité obligatoire, le régime de Vichy reprend un projet qui était déjà en discussion avant la guerre et qui aurait sans aucun doute rendu plus malaisé un changement d'identité.

Dans un rapport officiel publié en 1975, un haut fonctionnaire raconte une histoire pleine d'enseignements : « *Une équipe de jeunes Turcs à laquelle je participais, avait mis au point en 1938 un mirobolant projet de carte d'identité obligatoire des Français à partir de l'âge de 16 ou de 18 ans qui, à l'époque, aurait constitué un incontestable progrès en raison des moyens limités dont disposait la police pour lutter contre la criminalité. Au moment de présenter le décret à la signature du ministre, le secrétaire général du ministère de l'intérieur y renonça finalement, nous*

déclarant que, décidément, "il ne sentait pas la chose". Si M. Jean Berthoin avait eu "moins de nez" et se fût laissé convaincre par ses fringants collaborateurs, qu'en aurait-il été deux ans plus tard de la Résistance, les Allemands n'ayant naturellement rien de plus pressé, dès leur entrée dans Paris, que de faire main basse sur le fichier central de la carte d'identité des Français ? »

Les gouvernants néerlandais n'ont pas fait preuve de la clairvoyance de M. Berthoin. Dès les années 1930, ils avaient doté chaque citoyen d'un numéro d'identité signifiant. Tous les chiffres de ce numéro avaient une signification : commune d'origine, date de naissance, etc. Cette identification administrative centralisée et rigide, que des machines mécanographiques aidaient à gérer, ne laissait aucune chance à un changement d'identité. Dès leur entrée dans le pays, les nazis mirent la main sur le fichier central ainsi constitué et furent en mesure, avec une efficacité et une rapidité inconnues jusqu'alors, de repérer la population juive à exterminer. Les résultats obtenus sont éloquents : « *Sur une population estimée à 140 000 personnes, plus de 107 000 Juifs hollandais furent déportés et, sur ce nombre, 102 000 furent assassinés, soit un taux de mortalité d'environ 73 %. En France, où l'identification de la population était décentralisée et non homogène, avec un parc mécanographique en voie de constitution, sur 300 000 à 350 000 Juifs, près de 85 000 furent déportés, avec seulement 3 000 survivants, soit un taux de mortalité d'environ 25 %.* » [4].

4 L'alternative offerte par une informatique decentralisée respectueuse des libertés

17 En réaction à un « encerclement » des individus ne s'arrêtant parfois même qu'au delà des limites de leur corps, ont été élaborées deux approches complémentaires. La première, appelée « *privacy by design* », vise à intégrer le respect de la vie privée et des autonomies individuelles dès la phase de conception des systèmes informatiques. Sa mise en œuvre repose sur un ensemble de méthodologies telles que la « minimisation des données », c'est-à-dire le fait de ne produire que les données strictement nécessaires au traitement projeté, et la mise en œuvre de principes architecturaux visant à conserver les données au plus près des personnes ou, à tout le moins, à conditionner la possibilité technique d'exploitation distante des données à une action positive des personnes. La deuxième, appelée « *privacy by default* », vise à ce qu'un système informatique soit toujours initialement paramétré de façon à être le moins intrusif possible. Il revient alors à l'utilisateur de modifier ledit paramétrage et de lever certaines de ces protections, selon les services dont il souhaite bénéficier. Ces deux approches, élaborées dans la sphère nord-américaine [7], ont trouvé un terreau favorable en Europe. Outre qu'elles sont recommandées par toutes les autorités de protection des données, le futur Règlement européen sur la protection des données personnelles fait obligation aux responsables de traitements d'y recourir, même si cette démarche est loin d'être facile à mettre en œuvre face aux intérêts des gouvernements et des entreprises.

18 Comme l'Histoire l'a montré, les barrières juridiques ne sont pas opérantes pour empêcher un détournement de finalité : le pouvoir qui interdit une action peut être rapidement remplacé par celui qui l'autorisera. Tel a été le cas du FNAEG, initialement conçu dans le but d'identifier les récidivistes des crimes les plus graves. La régularisation a posteriori par le législateur, en juin 2016, des « recherches en parentèle » exigées par certains juges depuis 2000, dans lesquelles on s'attache à savoir si la trace biologique correspond à un parent d'une personne présente dans le fichier, a transformé celui-ci en « fichier des gens honnêtes ». En effet, la récidive des personnes présentes dans le fichier n'est plus la question ; seul compte le fait que suffisamment de personnes y soient présentes pour que l'on puisse en étendre la capacité d'identification, par affinité génétique, à l'ensemble de la population. De fait, l'extension en 2003 des prélèvements génétiques aux suspects d'atteintes aux personnes et aux biens (telles que le fauchage d'OGM)

a permis d'inclure dans le fichier un nombre significatif de personnes, susceptible de permettre l'identification indirecte de la majorité de la population.

Seules les barrières techniques peuvent offrir une protection effective contre les détournements 19
de finalité des systèmes informatiques. La principale consiste en la définition d'une architecture rendant impossible ces détournements [2]. D'autres modalités techniques, telles que la cryptographie à la main de l'usager, permettent d'empêcher les tiers d'avoir accès aux données, quel que soit l'endroit où elles sont stockées. L'apparition des outils numériques et des réseaux de communication instantanée doivent ainsi nous amener à repenser en profondeur l'ensemble des processus administratifs qui, en presque totalité, ont été pensés à une époque où ces réseaux et les moyens numériques n'existaient pas. Tel est le cas de l'authentification et du rôle qu'y joue la puissance publique.

Avant l'ère industrielle, les personnes se déplaçaient peu en dehors de leur groupe d'origine. 20
L'identité des personnes était donc une connaissance partagée, et son attestation s'effectuait par la reconnaissance par les familiers C'est ainsi que dans l'affaire Martin Guerre, jugée en appel à Toulouse en 1560, 300 personnes furent consultées, dont 280 ont déclaré que le prévenu n'était pas Martin Guerre et, pour certaines, l'ont correctement identifié comme étant Arnaud du Tilh. La tenue de registres ayant force probante quant à l'état civil des personnes, sous la forme de registres paroissiaux, pratiquée dès le Moyen-Âge, n'a été rendue obligatoire qu'au XVIe siècle par l'article 51 de l'ordonnance de Villers-Cotterêts, citant spécifiquement la finalité de la détermination du statut de majorité. La révolution industrielle et l'exode rural, en facilitant les déplacements et en conduisant au regroupement de masses anonymes au sein des grandes villes, ont fait apparaître pour l'État la nécessité de disposer d'une « chaîne de confiance » entre, d'une part, les personnes délivrant une preuve d'identité et, d'autre part, les personnes à même de l'utiliser. C'est ainsi que l'administration prit en charge le double rôle de concevoir des documents normalisés aussi peu falsifiables que possible, par l'usage de procédés techniques tels que le filigranage, les tampons en relief, etc., et de mettre en œuvre le processus de délivrance desdits documents. Pour autant, dans le cas où la personne en charge de la délivrance ne connaît pas personnellement le demandeur, se pose toujours la question de la confiance à apporter aux documents présentés à l'appui de la demande. Ainsi, une note rédigée en octobre 2011 à destination du cabinet de la Présidence de la République avança que près de 10 % des passeports biométriques délivrés en France les années précédentes seraient des faux, obtenus au moyen de documents d'état civil trop facilement falsifiables ; ces chiffres furent démentis par le ministère de l'Intérieur, qui refusa de communiquer ses propres estimations.

De même, quelle certitude peut-on avoir que le détenteur d'un document en est bien le titulaire légitime ? Une première contre-mesure s'appuie sur la rareté des documents : chacun n'étant censé posséder qu'un unique titre d'identité, la disparition de celui-ci est en général rapidement constatée par son titulaire, qui peut déclencher une procédure d'opposition. La date de péremption des documents vise également à limiter la durée des fraudes. Enfin, le recours à des procédés biométriques tels que la photographie a permis de réduire les cas d'usurpation.

Les titres d'identité que nous connaissons, ainsi que leur procédures de gestion, sont le résultat de l'adaptation aux techniques pré-numériques de ces préoccupations. Ces procédures incluent également un certain nombre de gardes-fous destinés à empêcher les détournements de finalités, tels ceux commis au cours de la Seconde Guerre mondiale. C'est par exemple le cas du stockage, sous forme papier uniquement et de façon décentralisée dans les préfectures, des demandes de cartes nationales d'identité. Ce mécanisme a été mis en place afin de prévenir la centralisation, dans un unique fichier, de l'ensemble de la population, incluant leur photo et leurs empreintes digitales. En cas de conflit, les préfets auraient alors le temps de détruire ou de mettre en sûreté des portions significatives de ce fichier. Ce garde-fou disparaît avec TES-2 mais, même sans cela, l'existence de scanners à haute résolution rend maintenant possible à un régime autoritaire

de numériser en quelques semaines l'ensemble des fiches cartonnées disponibles, réduisant le temps de prise de conscience du danger et la capacité des autorités locales à s'opposer à cette numérisation pour des raisons éthiques. De fait, toutes ces mesures de sauvegarde, ainsi que l'architecture générale des systèmes de gestion des titres d'identité, doivent être réévaluées à l'aune des techniques actuelles et envisageables dans un futur proche, et ce de façon régulière.

21 Afin de restreindre la capacité de régimes autoritaires à mettre en œuvre des « rafles assistées par ordinateur », les éléments d'identification propres aux personnes ne doivent pas être accessibles aux autorités de façon centralisée, que ce soit en base centrale ou délocalisées dans des administrations locales. Le principe de la conservation des données biométriques par les usagers eux-mêmes doit devenir la règle. Il a déjà été mis en œuvre dans le cas des passeports biométriques, qui embarquent les données biométriques des personnes au sein d'une puce insérée dans le document, ces données étant « signées » au moyen d'une clé de chiffrement que seul l'État possède. Pour autant, ces informations biométriques sont actuellement également répliquées dans la base centralisée TES-1, dont elles devraient donc être supprimées. Afin que de telles bases ne puissent pas être construites par recoupement, aucun service public ne devrait conserver de données biométriques d'authentification, telles que les photographies des personnes, au sein de leurs systèmes d'information. Ceci implique en particulier que les photographies servant à la création des cartes personnalisées ne soient jamais conservées au delà du moment où ces cartes sont mises en fabrication (permis de conduire, cartes Vitale, de réseaux de transport, etc.).

D'une façon plus globale, l'émergence des technologies numériques, au premier rang desquelles la cryptographie à clé publique, doit conduire à repenser en profondeur la question de l'identité des personnes et des moyens de s'en assurer. Le rôle actuel de l'État comme autorité de délivrance des titres tient à sa capacité supposée à s'assurer de l'identité des demandeurs. Pour autant, d'autres systèmes plus décentralisés sont possibles, dans lesquels les familiers d'une personne attesteraient de cette identité en « signant » cryptographiquement les documents de leurs connaissances. Un tel mécanisme est déjà employé au sein des communautés d'usagers de la cryptographie pour signer les clés cryptographiques de ses connaissances et ainsi augmenter leur niveau de confiance vis-à-vis de tiers. Une telle architecture correspondrait en fait à un retour aux fondements de l'identité, en tant que connaissance partagée par les membres d'une communauté. Elle pourrait éviter le recours aux informations biométriques, d'usage délicat car non révocables. Cependant, elle aurait pour inconvénient majeur de rendre plus difficile l'établissement de faux papiers, de multiples personnes devant alors se porter garantes du détenteur du titre d'identité, s'exposant avec lui.

22 L'irruption des technologies numériques doit amener à reconsidérer l'équilibre entre libertés et sécurité. Alors que les capacités de traitement toujours croissantes et la collecte massive de données peuvent conduire à un contrôle accru des personnes, il convient de repenser l'architecture des systèmes de gestion de l'identité à l'aune de ces nouvelles modalités techniques, en conformité avec les valeurs promues par le mouvement émergent des « *civic tech* ». Ces architectures doivent être conçues dans l'objectif de rendre techniquement impossible tout détournement de finalités, selon le principe de « *privacy by design* », fût-ce au prix du maintien d'une capacité de fraude documentaire. Cette capacité, offerte à un nombre suffisant d'acteurs, doit à l'inverse être une caractéristique intrinsèque souhaitable des systèmes de gestion d'identité, en tant que garde-fou face à des convulsions historiques telles que les sociétés modernes en ont déjà connues.

Références

[1] I. About et V. Denis. *Histoire de l'identification des personnes*, La Découverte, Paris, 2010.

[2] T. Antignac et D. Le Métayer, « Privacy by Design : From Technologies to Architectures », in B. Preneel et D. Ikonomou, eds., *Privacy Technologies and Policy : Second Annual Privacy Forum*, APF 2014, Athènes, Grèce, 20–21 mai 2014. Springer International Publishing, pp. 1–17, DOI 10.1007/978-3-319-06749-0_1.

[3] J.-M. Berliere , P. Fournie, *Fichés ?*, Perrin, Paris, 2011.

[4] E. Black, *IBM et l'holocauste*, Robert Laffont, Paris, 2001.

[5] L. Bonelli, *La France a peur. Une histoire sociale de l'insécurité*, La Découverte, Paris 2010.

[6] C. Castelluccia et D. Le Métayer, « NOTE D'ANALYSE – Titres électroniques sécurisés : la centralisation des données biométriques est-elle vraiment inévitable ? Analyse comparative de quelques architectures gmr, Rapport de recherche, INRIA Grenoble – Rhône-Alpes, février 2017. Voir : `https://hal.inria.fr/hal-01467902` .

[7] A. Cavoukian, « Privacy by design – The 7 foundational principles », IPC office, province d'Ontario, 2011. Voir : `https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf` .

[8] Conseil constitutionnel, Décision n° 2012-652-DC du 22 mars 2012. Voir : `http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html` .

[9] F. Gallouedec-Genuys, P. Lemoine, *Les enjeux culturels de l'informatisation*, La Documentation française, Paris, 1980.

[10] V. Gautron, gml Usages et mésusages des fichiers de police », in *Déviance et Société*, vol. 37, n° 1, 2013.

[11] C. Hoffsaes, A. Vitalis, « Les hommes-numéros », in *La Recherche*, n° 278, juillet/août 1995.

[12] A. Mattelart, *L'invention de la communication* La Découverte, Paris, 1994, pp. 255–308.

[13] A. Mattelart, A. Vitalis, *Le profilage des populations – Du livret ouvrier au cybercontrôle*, La Découverte, Paris, 2014.

[14] G. Noiriel, *L'identification – Genèse d'un travail d'État*, Belin, Paris, 2007.

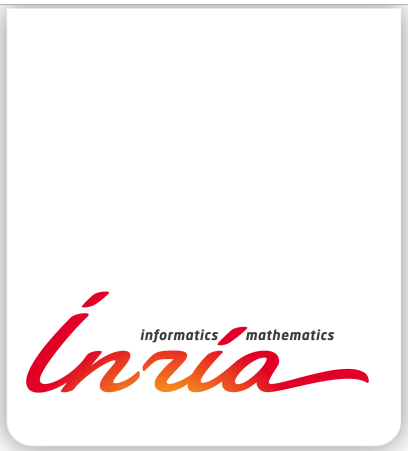
[15] F. Pellegrini, « La biométrie des honnêtes gens, reloaded », blog personnel, novembre 2016. Voir : `http://www.pellegrini.cc/2016/11/la-biometrie-des-honnetes-gens-reloaded/` .

[16] P. Piazza, *Aux origines de la police scientifique – Alphonse Bertillon, précurseur de la science du crime*, Karthala, Paris, 2012.

[17] G. Poupard, H. Verdier, « Audit du système "Titres électroniques sécurisés" », 13 janvier 2017. Voir : `http://mobile.interieur.gouv.fr/content/download/100011/786238/file/rapport-commun-public-tes-13-01-20172.pdf` .

[18] A. Vitalis, *Informatique, pouvoir et libertés*, Economica, Paris, 1988, pp. 77-90.

[19] A. Vitalis, *L'incertaine révolution numérique*, ISTE, Londres, 2016, pp. 33–49.



RESEARCH CENTRE
BORDEAUX – SUD-OUEST

200, avenue de la Vieille Tour
33405 Talence Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399